УДК 621.396.946.2 (075.8)

СИСТЕМЫ УСЛОВНОГО ДОСТУПА В СЕТЯХ ЦИФРОВОГО ТЕЛЕВИЗИОННОГО ВЕЩАНИЯ

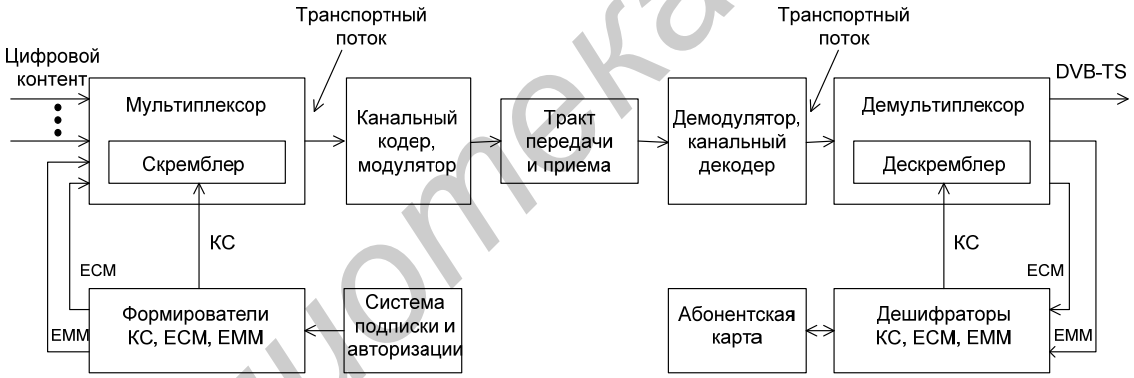
Э.Б. ЛИПКОВИЧ, А.В. ЛЕВИЦКИЙ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь

Рассматриваются особенности построения систем условного доступа (СУД) в сетях спутникового и наземного вещания, которые призваны защитить мультимедийный материал правообладателя от несанкционированного приема и использования.

Ключевые слова: защита информации, несанкционированный прием, контрольное слово, шифрование контента.

Сущность работы СУД состоит в искажении закрываемой информации настолько, чтобы ее просмотр или перехват секретных материалов стали невозможными без применения специального декодирующего устройства при приеме и оплаты за предоставляемые услуги [1]. В цифровых системах мультимедийного вещания защита информации осуществляется за счет безызбыточного кодирования (скремблирования) данных на стороне передачи и их восстановления в дескремблере на стороне приема (рис. 1).



ECM – Entitlement Control Message – сообщение контроля доступом
EMM – Entitlement Management Message - сообщение разрешения на доступ

Рис.1. Структурная схема организации условного доступа

Согласно рекомендациям DVB, устройства и процедуры скремблирования установлены едиными для всех сетей спутникового, наземного и кабельного вещания. Однако структура построения скремблера и алгоритм его работы являются неизвестными для операторов сетей ТВ-вещания, поскольку право на производство устройств скремблирования/дескремблирования отдано определенным компаниям (Scopus, Tandberg, NDS, Scientific Atlante).

В системах DVB скремблер управляется кодовой комбинацией или по-другому контрольным словом (КС). Периодичность смены КС составляет 4…5 с, что исключает прочтение передаваемой информации путем перебора ключей. На приемной стороне дескремблер управляется тем же контрольным словом, которое для безопасной его доставки всегда шиф-

руется при передаче. Способ шифрования КС устанавливается вещателем сети и регистрируется в ETSI. Шифрование КС осуществляется достаточно сложным сеансовым (долговременным) ключом с продолжительностью его действия несколько недель, месяц или более. Набор долговременных ключей для их смены ограничен. Это связано с небольшим размером энергонезависимой памяти абонентской карты (смарт-карты), хранящей эти ключи. Тактика обновления этих ключей в карте определяется оператором сети и производится подачей на декодеры специальных команд.

В процессе восстановления закрытых программ на приемной стороне осуществляется идентификация принятого способа кодирования, расшифровка КС, аутентификация и авторизация абонентов с установлением их прав на доступ к платным услугам и др.

С общих позиций рассматриваемая система условного доступа соответствует симметричной модели криптографии, в которой на стороне передачи и приема используется один и тот же секретный ключ для выполнения обратимых преобразований. В рамках этой модели создано большое число СУД с аппаратными и программными способами криптозащиты, которые пригодны также для интерактивных сетей. С точки зрения информационной безопасности аппаратная реализация криптоалгоритмов имеет преимущества перед программной, однако уступает последней по стоимости и скорости обработки информации.

К числу программных способов шифрования контента, применяемых в мобильных, кабельных, IPTV и Интернет-сетях, относятся системы криптозащиты Verimatrix Content, Secure, Irdeto, Nagravision, Conax Contego. Этим системам присущи различные подходы по обеспечению информационной безопасности и мерам защиты ядра СУД от возникающих угроз. Они отличаются архитектурой построения, числом используемых ключей, методами шифрования, сложностью алгоритмов и программного обеспечения.

На стороне пользователей применяются как карточные, так и бескарточные способы восстановления переданной информации. Бескарточный способ дешифрации предлагается компаниями Verimatrix, Irdeto, Conax Contego и Access-Ora, в которых предусматривается использование специального программного обеспечения и секретных алгоритмов. Считается, что для сетей с повышенным риском перехвата информации предпочтительнее карточный вариант, хотя взлом программного чипсета представляется более сложным, чем взлом смарт-карты. Наличие в сети обратного канала позволяет существенно усилить механизмы защиты контента от атак на предоставляемые услуги и снизить вероятность взлома СУД.

Список литературы

1. *Липкович Э.Б., Кисель Д.В.* Проектирование и расчет систем цифрового спутникового вещания. Мн.БГУИР, 2006.